FortiADC - 2FA Script Deployment Guide

Version 5.4.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 20, 2020
FortiADC 5.4.1 2FA Script Deployment Guide
01-540-600000-20200220

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-09-24	Initial release.
2018-10-18	Cannot generate tagged PDF (MadCap bug); target updated.

Introduction

FortiADC 2FA provides stronger security for authentication when the client uses a FortiADC local account to login to the Virtual Server (VS). In addition to a username and password, you will need the correct token (given by phone) to confirm your login into the VS.

Before you begin, you must do the following:

- Configure "User Authentication Settings" on the Virtual Server
- Download the FortiToken or Google Authenticator app on your mobile phone.
- Ensure that the time on the FortiADC and the mobile phone are the same.

Deploying FortiADC-VM on 2FA Script

Step 1: Create a tokengroup

FortiADC-VM # config system tokengroup

FortiADC-VM (tokengroup) # edit 1

FortiADC-VM (1) # end

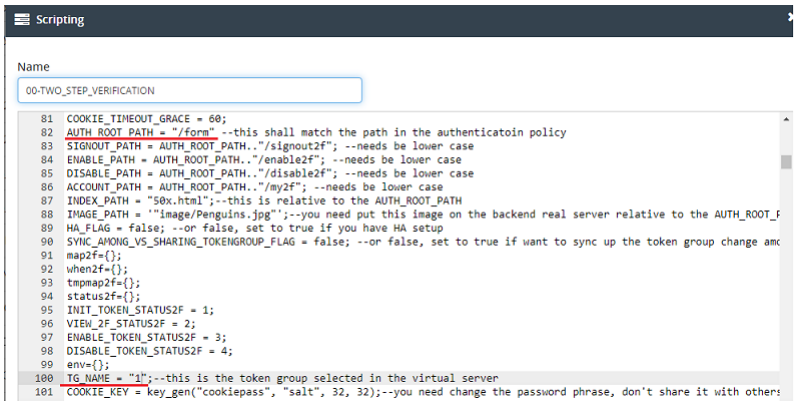
FortiADC-VM #

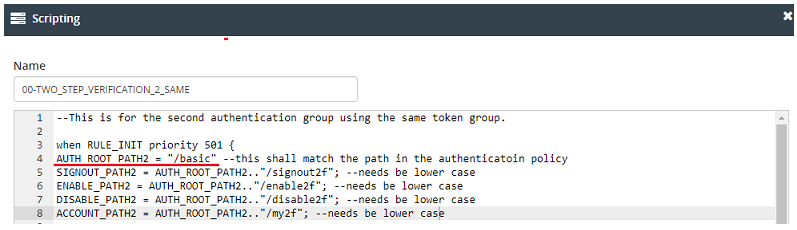
Step 2: Configure the pre-defined script

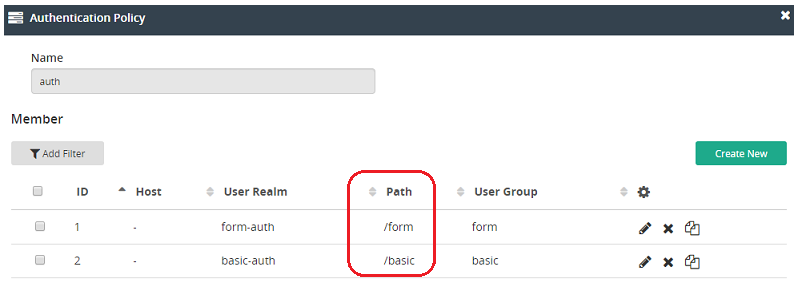
1. TWO_STEP_VERIFICATION
2. TWO_STEP_VERIFICATION_2_SAME

The keys of the parameter:

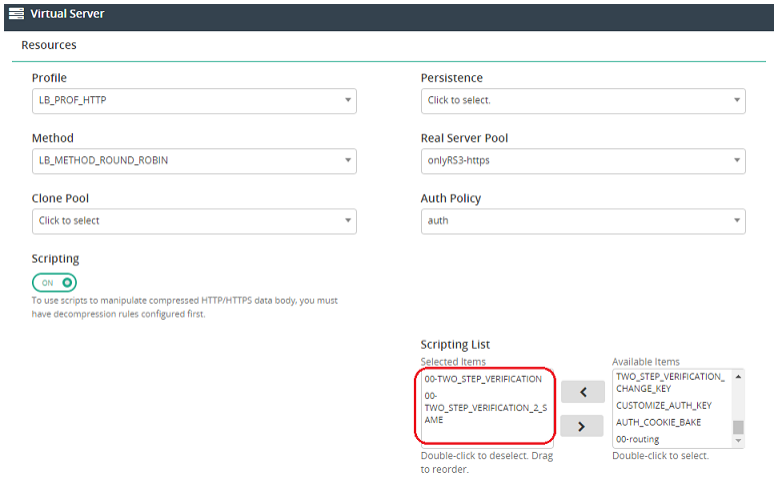
- AUTH_ROOT_PATH—The authentication folder under "User Authentication" settings. One is for the form method and the other for the basic.
- TG_NAME —Use the tokengroup entry from Step 1.







Step 3: Link these scripts to the VS



Step 4: Link the tokengroup to the VS.

FortiADC-VM # config load-balance virtual-server

FortiADC-VM (virtual-server) # edit http-60

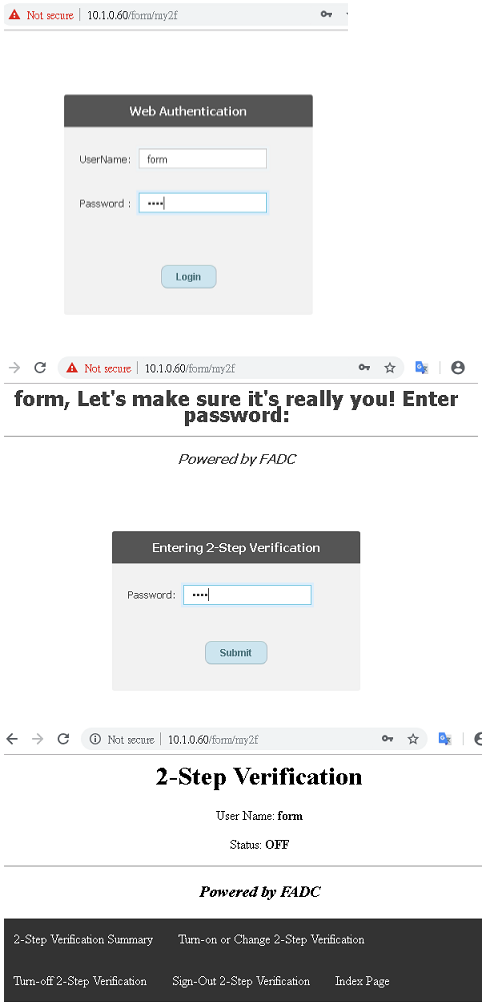
FortiADC-VM (http-60) # set token-group-list 1

FortiADC-VM (http-60) # end

FortiADC-VM #

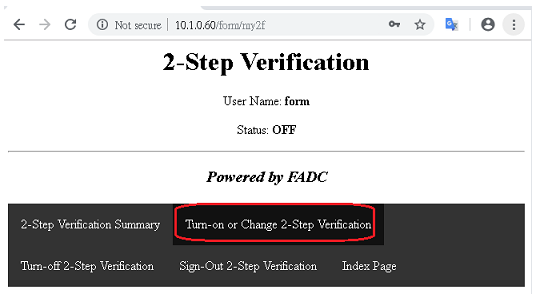
Step 5: Access the my2f page from client.

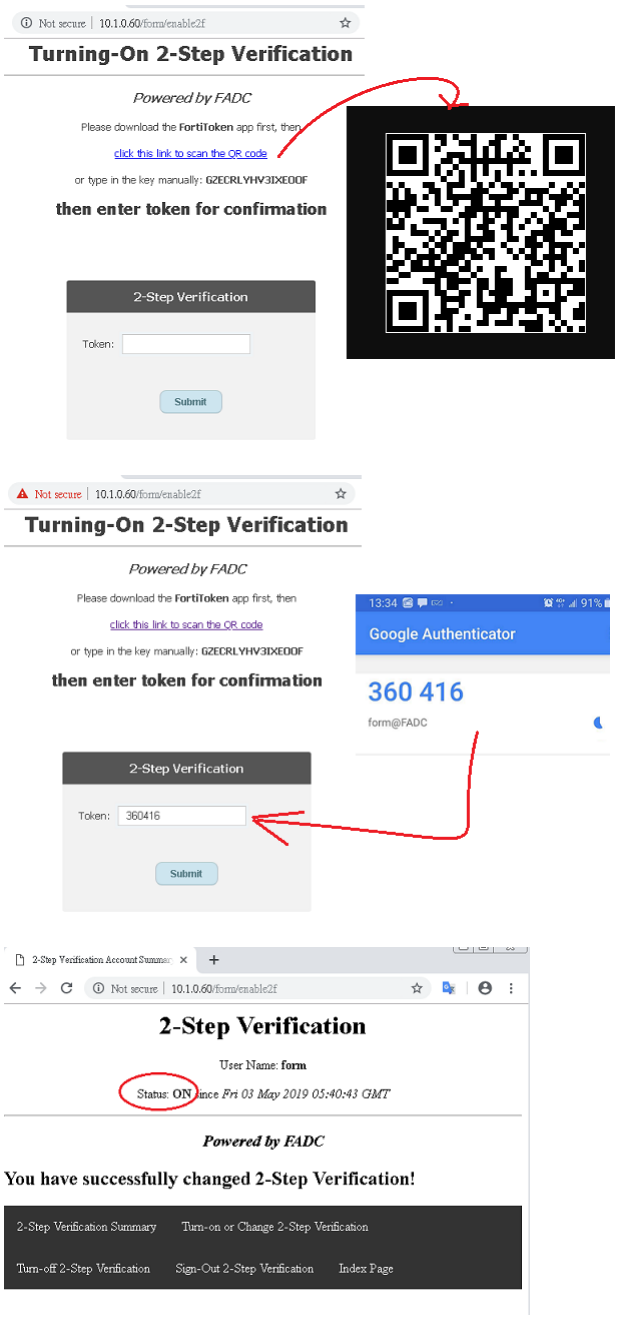
1. Access the VS page under AUTH_ROOT_PATH/my2f and input the correct user/passwd.
2. Input the password again.
3. You will see the 2FA summary page.



Step 6: Try to turn on the 2FA feature by user account.

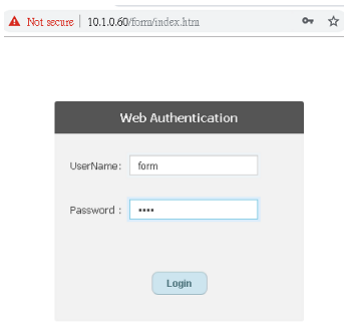
1. Click the **Turn-on or Change 2-Step Verification** to turn on the feature.
2. Will require to scan a QR code to input the information on the APP.
3. Input the token for confirmation.
4. Check if the status is ON on the my2f page.

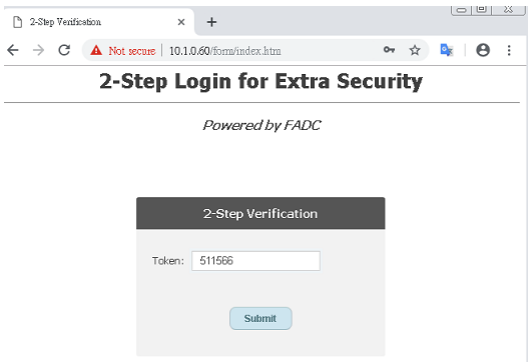


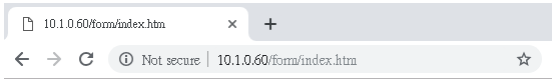


Step 7: Verify the 2FA feature is enabled under AUTH_ROOT_PATH folder

1. Access the page http://VS/form/index.htm
2. Input the username and password.
3. Input the token for the 2FA verification.
4. You will see the index.htm content.







Test FORM-HTML Test